fundamental:
mobile forensic informatic science in court

a short essay by secinfo

… retyping the rules!

Criminological forensics is primarily about finding evidence that withstand in court. This essay is based on german law system and german proof survey process. Principle are similar in constitutional states all over the world.	about
Computer forensics means of a special backup of data carriers or data in general to provide a certain proof. This evidence is usually also submitted to a court so it is fundamental that the data during the analysis under no circumstances be changed. If only a single byte is changed, the evidence in court is no longer meaningful. This has been a fundamental principle in the last 50 years.	today
Really? What's about mobile forensic? How to handle devices like Apple iPhone or Samsung Galaxy coming with a modern iOS or Android? Is mobile forensice a kind of computer forensic science? Of course it is!	about mobile devices

But what makes the different to server and desktop computer? Both own processor, mainboard, display, keybord rsp. virtual keyboard and permanent memory, a harddisk or an eprom. Here is the difficulty: You cannot remove the permanent memory from the mobile device without using a soldering iron or a milling machine.

Removing the mobil device storage means: handy is irretrievably destroyed. The problem is due to the design.

This could be an alternative method in cases of murder and heavy robbery but in most cases, the destruction is not considered.

… and here begins the problem

First sentence:

The forensic scientist can not usually remove the memory from the device.

Second sentence:

The forensic scientist must turn on the device to secure data.

Third sentence:

Turning the device on the forensic scientist changes the data to be backed up.

the supposed no go

Sentence number 3 violates the procedural rules. These rules are:

procedural rules

- Documentation of each executed step.
- The data to be backed up (if possible) must remain unchanged during the backup process and all other processes.
- The integrity of the data must be secure at all times.

All of these requirements must be evidenced by the court. Sounds simple - but it is not.

First: why are these three points so important in the criminal proceedings?

The question of traceability and reproducibility is central to a fair procedure. Only in this way is it possible for the defendant to assess the evidence, only then is it possible for the defender to obtain, for example, a counter-opinion.

However, when testing mobile devices like handy, we generally can not prove the integrity of the examination subject. The forensic scientist can not create an image using dd, he isn't able to generate a thinful hash value because the device is working.

always, if you think it could not get worse

The forensic scientist does not just turn on the device, he puts it into download mode, the usb debugging mode or he is rooting the device. He may even remove the access barrier first – summary: The data on the device has been changed. More: the data was changed irreversibly.

So what do we have to say? This proof is unsuitable? Such a modified means of proof is not permitted?

Note:
A modified mobile phone is not a fake proof. A SMS from a rooted smartphone remains in its content and thus as evidence unchanged. The same applies to almost all user data.

Most things that forensics seeks are untouched during usb-debugging, rooting or password hacking.

But what will the judge say? How can it be possible to convince the judge of the factual integrity of the proof?

I will show you how:

Construction of the expert report

First of all we note:

- every time we turn on a cellphone we change it's data.
- every time we examine a mobile phone, the phone changed its data status permanently

Fact.

- user data eg. contacts, SMS, WhatsApp, images, videos, websites and email will not be changed (in flight mode or into a Faraday cage: no remote control)
- however, technical data is changing (logs, connections, temp data …). This also applies if the flight mode is set.

Fact too.

Of course, this information should not be withheld from the court. After the examination order and the description of the examination object, the expert must name the operating status of the device.

Step by step.

- Our examination object is up and running, accu has more than 50%. Flight mode is activated (or the device is in a Faraday cage), no SIM card inserted.

- Howto back up data for the procedure? What methods are there? You will have:

- logical method (backup or app).
- physical method (with or without rooting)
- proprietary (most simple cellphones)
- photographically over the display

- *All methods to be used depend on the device in a single case. Two devices can be the same externally, have the same name and still use different chipsets (and so they are diffrent).*

!

logical via app

- *Logical data backup via agent app. Logical backup means backing up the individual objects such as sqlite-tables or indexes.* Copy agent app to the smartphone and the games begin.

  → example A:
  expert report (per default)
  logical method (agent app)
  OS: Android

logical backup

- Creating a *logical backup* is the most easiest method to copy and save smartphone data – if it works. It should be fine examining i-Devices (with code) and all android phones.

  Restriction: you do not get all user data, no OS data eg. data in databases or tables.

  → example B:
  expert report (per default)
  logical method (backup)
  OS: Android (also iOS)

- Examining a device *physical:* Physical backups rely on the Operating System to make a copy of the physical files like data files, log files, control files that comprise the database.

  You'll only get the files from the data partition.

  The physical backup has only limited rights, the backup does not contain all files.

  (with or without rooting)

  Learn more about the different between physical and logical extraction:
  https://www.usenix.net/legacy/publications/library/proceedings/osdi99/full_papers/hutchinson/hutchinson.pdf

  → example C:
  expert report (per default)
  physical
  OS: Android, older iOS and other

physical

- rooting the android
  To root = to otain administrator rights
  Some files in adroid systems require root privileges to run. Simplified: root may everything. Root could backup (nearly) erverything.
  But: rooting influences the safety. Internet banking can become impossible, the manufacturer's warranty expires (civil effects)

  → example D:
  expert report (per default)
  special report concerning root process and its impact
  OS: Android (Unix)

  Note: iOS is a unix devirate, it comes from free bsd. Of course it can be rooted in principle. A cydia jailbreak is a rooting process.

rooting

- Hacking the access code to remove an encryption. Many smartphones are protected with an access code. For data backup, this must be known or removed.

  → information E:
  Information for the report - what has to be submitted to the court?

hacking

keywords

forensic report

The keywords are accuracy and traceability.

Be carefull – be exactly.

forensic reports on mobile devices

Compared to traditional forensic expertise, forensic reports on mobile devices must provide accurate and final information about data that may be altered by the backup process.
The documentation has to be done specifically with a high degree of detail.
Generically oriented forensic reports should or will not be recognized in court.
While index and content can be marked as unchanged in the report, it is possible that the data on the dates (timestamps) are no longer correct. The date and time may only be displayed correctly on a running system. The entry could refer to another time zone. And the reference is missing because the device is no longer online or off.

I would like to give you an example of the term specific: We have just backed up data on an Android device and are looking at the SMS.
what is changed, what is integer? The backup file should contain a sqlite database with data from the sms as well as a reference to the binary program file, it's version and so on.

Note: in important cases, the device should be returned after a final judgment. An expert report with a counter-opinion can best be compiled from the original material.

!

A) expert report (per default)

→ logical method (agent app)

OS: Android

	points of expertise	Data will be changed	kind of data	Significant for integrity of the evidence
1	examination order	n		n
2	description of the examination object	n		n
3	status	n		n
4	Flight mode/ Faraday cage	y	kills all connections	n
5	Switching USB-Debugging „on“	y	USB Subsystem, adb, access rights for the examination computer	n
6	Connect Android to the exam PC – recieving system data **Befehl** / **Information** adb shell getprop ro.product.manufacturer – Gerätehersteller adb shell getprop ro.product.model – Gerätemodell adb shell getprop net.hostname – Gerätename adb shell getprop ro.build.version.release – Android-Version adb shell getprop gsm.operator.alpha – Netzbetreiber adb shell getprop ro.serialno – Geräteseriennummer adb shell getprop ro.runtime.firstboot – Zeit des letzten Starts adb root – Root-Berechtigung	y	Settings: permissions to „allow“	n
7	Copy agent app to the smartphone	y	The code (bin)for the extraction is on the phone	n
8	Creating a list of touched apps, maybe: com.android.calendar com.samsung.android.app.memo com.android.stk com.android.nfc com.samsung.SMT com.google.android.music com.google.android.apps.maps com.google.android.apps.docs com.android.browser.provider	n for all		n

	com.sec.factory.camera com.sec.android.widgetapp.digitalclock com.samsung.android.email.provider com.sec.di.SmartSelfShot com.android.providers.telephony com.google.android.googlequicksearchbox com.android.providers.calendar com.android.externalstorage com.android.mms com.android.contacts com.sec.android.omc com.sec.android.gallery3d			
9	Summary: unchanged sqlite databases, textbased data files. No files, no images, no videos, no audios			n
10	accuracy and traceability: documented			
				.

B) expert report (per default)

→ logical method: backup

OS: Android

	points of expertise	Data will be changed	kind of data	Significant for integrity of the evidence
1	examination order	n		n
2	description of the examination object	n		n
3	status	n		n
4	Flight mode/ Faraday cage	y	kills all connections	n
5	Switching USB-Debugging „on“	y	USB Subsystem, adb, access rights for the examination computer	n
6	Connect Android to the exam PC – recieving system data	y	Settings: permissions to „allow“	n
7	Sending backup request over adb interface adb backup –all –f c:\backup.ab	y	user reaction required on the device „Backup my data“	n
8	backup runs via system services	n		n
9	Summary: a backup container in *ab format			n
10	accuracy and traceability: documented			
				.

C) expert report (per default)

→ physical without rooting

OS: Android

	points of expertise	Data will be changed	kind of data	Significant for integrity of the evidence
1	examination order	n		n
2	description of the examination object	n		n
3	Status on or/and off	y	Log, temp	y
4	Flight mode/ Faraday cage	y	kills all connections	n
5		y	U	n
6	Connect Android to the exam PC – recieving system data	y	Settings: permissions to „allow"	n
7	Downgrading apps (general)	y	binaries	n
8	Downgrading Google Chrome	y	App-prog/binaries	n
9	Downgrading Instagram	y	App-prog/binaries	n
10	Downgrading WhatsApp	y	App-prog/binaries	n
11	Updating after downgrade	y		n
12	7 -11	y	Logs and dates of installed apps	y
13	System time	y	all data that uses relative time (relative to system time)	y
14	Bootlog and similar files. It's likely to have to reboot the android several times to back up all the data	y	Log entries	y
10	accuracy and traceability: documented			

D) expert report (per default)

→ rooting

OS: Android

	points of expertise	Data will be changed	kind of data	Significant for integrity of the evidence
1	examination order	n		n
2	description of the examination object	n		n
3	Status on or/and off	y	Log, temp	y
4	Flight mode/ Faraday cage	y	kills all connections	n
5		y	U	n
6	Connect Android to the exam PC – recieving system data	y	Settings: permissions to „allow"	n
7	initiate the root process via PC or app	y	Change of the complete system by user conceivable change of administrative rights Soft-Brick possible Hard-Brick possible later civil law issues: loss of warranty	Y
	+ physical extraction (C with rooting)	y		y
10	accuracy and traceability: documented			

E) hacking - beware the dog!

An information - no suggestion for a forensic report

OS: iOS

Example: iPhone 7, iOS 11, lock code of the screen unknown (device is technically ok)

Information for the report - what has to be submitted to the court?

	points of expertise	Data will be changed	kind of data	Significant for integrity of the evidence
1	examination order	n		n
2	description of the examination object	n		n
3	Status on, unknown lock code, unknown length			
4	Flight mode/ Faraday cage (if possible)	y	kills all connections	n
5	Perform various attacks to overcome the lock code	y	concerns the safety of the entire device, ultimately, it affects the integrity of all data	n
6	Vulnerabilities published by a process will pose a significant risk to all users of the device type in the future		risk for all OS	
7	Many hacks are not suitable for publicity. there will inevitably be divergences between information gathering and a transparent procedure.	y		Y Evidence ban?
8	opening external sources	n	Cloud computing, additional memory like SD-Cards	Y Evidence ban?
9	Destruction of the hardware to get detailed information	y	all data	n
10	accuracy and traceability: possibly not sufficiently documented			

Written by

secinfo

PS: english not okay? Sry, I'm a kraut.